

附件一

經濟部能源署使用戶政資料管理計畫

一、法律依據及使用目的

(一)法律依據

- 1.石油管理法第三十六條第一項第二款規定，石油基金用途包含偏遠地區、原住民族地區及離島地區石油設施、運輸費用之補助及差價之補貼。同條第二項明定前項第二款補助、補貼對象、範圍及相關事項之辦法，由中央主管機關定之。經濟部並據以訂定偏遠與原住民族及離島地區石油設施及運輸費用補助辦法。
- 2.偏遠與原住民族及離島地區石油設施及運輸費用補助辦法（以下簡稱補助辦法）第四章（家用桶裝瓦斯差價補助）之規定。
- 3.依經濟部中華民國 104 年 7 月 1 日經能字第 10404603090 號公告，將前揭家用桶裝瓦斯差價補助業務委任予能源局（112 年 9 月 26 日改制為能源署）並委辦直轄市暨縣（市）政府辦理。

(二)使用目的：經濟部能源署（簡稱能源署）依前揭法規取得受補助地區民眾之戶政資料後，載入能源署資訊系統，供鄉（鎮、市、區）公所辦理偏遠與原住民族地區家用桶裝瓦斯差價補助業務。

二、適用機關及業務範圍

(一)適用機關：本管理計畫適用對象為能源署，以及補助辦法適用地區之鄉（鎮、市、區）公所。其中次年度補助辦法適用地區，依補助辦法第四條規定，由經濟部於每年 9 月底前公告。

(二)業務辦理範圍及對象：

1.能源署：

由能源署統一向內政部戶政司索取偏遠與原住民族地區戶政資料。並由能源署自內政部戶政資訊電子閘門系統檔案傳輸作業，批次下載戶政資料原始檔，進行資料解密後載入承商建置之資訊系統，提供鄉（鎮、市、區）公所至該資訊系統辦理民眾申請資料與戶政資料核對作業，並辦理列印與更新補助名冊作業，簡化差價補助行政作業。

能源署依政府採購法，將資訊系統建置及維運委由承商辦理並簽訂契約，承商僅得維護管理資訊系統，並協助辦理資訊系統相關個資安全與資訊安全管理事宜，並無法存取與戶政資料應用相關之功能與資料。能源署並依契約書規定邀請外部專家學者辦理期中、期末審查會議持續審核承商之適任性。

2.鄉（鎮、市、區）公所：

依補助辦法第三十四條透過前揭能源署資訊系統辦理申請民眾戶政資料核對及登錄作業，並利用該資訊系統彙整民眾申請資料後產製相關撥款清冊及核銷報表。公所可利用該資訊系統產製包含家戶成員姓名(已遮罩)、身分證字號(已遮罩)、地址、戶號、人口數、補助桶數、補助金額等資料之補助名冊紙本，請村(里)辦公處協助核對申請者身分，惟因該補助名冊之姓名與身分證字號個人資料皆已遮罩去識別化，村(里)辦公處僅得以初步比對並彙整民眾申請資料後，交由公所辦理後續戶政資料核對及申請審查核可作業。

前述村（里）辦公處藉由鄉（鎮、市、區）公所提供補助名冊紙本（已遮罩去識別化），僅得以姓名頭尾字元及身分證部分字元作初步比對並協助鄉（鎮、市、區）公所彙集民眾相關申請資料，並無法實際接觸可識別個人資料之戶政資料。而直轄市、縣（市）政府係督導轄內鄉（鎮、市、區）公所辦理差價補助業務執行情形，並將轄內業務辦理進度及經費支用情形函報能源署，並未實際接觸戶政資料。

- (三)資料應用範圍：能源署向內政部申請之偏遠與原住民族地區民眾之個人戶籍資料，係載入資訊系統，供鄉（鎮、市、區）公所造具補助名冊（個人資料已遮罩去識別化）、補助資格核對，家戶人口統計、補助費用核算與撥付、補助經費之核銷、補助資料彙整、統計。

三、專責人員管理

- (一)由能源署專責人員（即為各機關應用戶役政資訊電子閘門作業申請表上所載明之專責人員）辦理安全維護事項，並造冊列管所有使用、查詢戶籍資料人員等相關管理措施。能源署專責人員異動後應於7日內函知內政部。
- (二)能源署專責人員應每年至少接受3小時以上資通安全專業或資安職能訓練課程。

四、人員權限管理方式

使用資訊系統應用戶政資料，管理者及一般使用者應符合下列規範：

- (一)資訊系統之帳號類型區分為4類，即直轄市、縣（市）政府、鄉（鎮、市、區）公所、能源署、承商，其各帳號類型再依權限劃為管理者與一般使用者等2類使用者，若非屬差價補助業務相關人員不得申請帳號。
- (二)資訊系統之帳號與密碼，其通知過程應具保密措施，防止被竊視及竊取。
- (三)資訊系統之管理者及一般使用者不得使用非本人申請之帳號，帳號不得交接予他人，且不得和他人共用。
- (四)資訊系統帳號應每三個月更換密碼，且最近3次內不得重複，密碼長度至少12碼以上，須包含數字及英文並區分大小寫及特殊符號，使用者密碼應妥善保管，避免他人知悉。

- (五)資訊系統應限制使用者連續登入密碼失敗之次數最多為3次，超過3次即將帳號鎖碼，經申請核准後，即可由管理者解鎖帳號。
- (六)資訊系統管理者之帳號管理作業，基於分層制度應採二層管理，即由能源署辦理直轄市、縣（市）政府、鄉（鎮、市、區）公所、能源署承商等機關之資訊系統管理者帳號新增、異動、停用、審查等帳號管理作業。
- (七)資訊系統管理者之帳號新增或異動須經申請，直轄市、縣（市）政府、鄉（鎮、市、區）公所、能源署承商等機關之申請者，應向能源署申請核可後，由能源署辦理各機關資訊系統管理者帳號新增與異動作業。
- (八)資訊系統管理者之職務異動，直轄市、縣（市）政府、鄉（鎮、市、區）公所、能源署承商等機關，應於職務異動前或當日，向能源署申請辦理資訊系統管理者帳號停用，至遲於職務異動當日停用其帳號。
- (九)資訊系統一般使用者之帳號管理作業，由各機關資訊系統管理者辦理，即由直轄市、縣（市）政府、鄉（鎮、市、區）、能源署承商等各機關資訊系統管理者，辦理機關內部資訊系統一般使用者帳號新增、異動、停用、審查等帳號管理作業。
- (十)資訊系統一般使用者之帳號新增或異動須經申請，直轄市、縣（市）政府、鄉（鎮、市、區）公所、能源署承商等機關之申請者，應向機關內部權責主管申請核可後，由機關內部之資訊系統管理者辦理資訊系統一般使用者帳號新增與異動作業。
- (十一)資訊系統一般使用者之職務異動，直轄市、縣（市）政府、鄉（鎮、市、區）公所、能源署承商，應於職務異動前日，向機關內部資訊系統管理者申請辦理資訊系統一般使用者帳號停用，至遲於職務異動當日停用其帳號。
- (十二)除鄉（鎮、市、區）公所因受理差價補助業務民眾申請之需要與能源署因系統維護之需要外，其餘帳號類型之資訊系統使用者，其存取權限不得涉及應用內政部之民眾個人戶籍資料，且鄉（鎮、市、區）公所亦僅得存取所轄地區民眾個人戶籍資料。
- (十三)資訊系統之管理者應定期每半年辦理帳號清查，檢視使用者權限，並廢止重複、閒置、職務調整、離職及退休者帳號。
- (十四)資訊系統將以日誌記錄各類使用者利用資訊系統應用戶政資料之作業行為，並將此紀錄保存至少5年。
- (十五)申請戶政資訊連結作業之能源署權責主管、能源署專責人員與能源署承辦人應於職務異動後7日內，函知內政部並副知經濟部。

五、檔案存放管理及銷毀程序

- (一)批次取得戶政資料管制措施

- 1.由能源署自內政部戶政資訊電子閘門系統檔案傳輸作業，批次取得戶政資料原始檔後，除將資料載入資訊系統外，不得對資料進行其他應用或是以其他可攜式儲存媒體存取或傳送戶政資料。
- 2.戶政資料之應用，僅限於由能源署專責人員，將戶政資料載入資訊系統，由資訊系統利用戶政資料協助鄉（鎮、市、區）公所，依補助辦法第四章規定之業務範圍進行造具補助名冊、補助身分核對、家戶人口統計、補助費用核算、補助經費之核銷、補助資料彙整、統計等戶政資料之應用與產出。
- 3.鄉（鎮、市、區）公所利用資訊系統相關之戶政資料應用與產出，其資訊系統已自動將所有個人資料進行遮罩，以保障個資安全。
- 4.經由資訊系統對戶政資料應用與產出之資料，雖已經將個資進行遮罩，但各鄉（鎮、市、區）公所仍應辦理個人資料安全維護內部稽核，並留存稽核紀錄，以落實資料安全之維護。
- 5.村（里）辦公處依補助辦法規定之業務範圍，僅得協助鄉（鎮、市、區）公所發放和繳回補助名冊，不得有其它應用戶政資料之行為，鄉（鎮、市、區）公所亦應盤點補助名冊數量，確保補助名冊沒有缺漏。
- 6.直轄市、縣（市）政府依補助辦法規定之業務範圍，僅得利用資訊系統彙整轄下鄉（鎮、市、區）公所辦理差價補助業務相關費用，並且辦理帳務核銷、監督鄉（鎮、市、區）公所業務辦理情形、查核與稽核鄉（鎮、市、區）公所帳務與個人資料安全內部稽核紀錄，無權限得以進行任何戶政資料相關之應用與產出。
- 7.資訊系統之資料庫，應予以權限控管，非能源署指派之專員（即為經能源署指派之署內人員或承商人員），不得檢視和維護資料庫內容。
- 8.能源署指派之專員，應於每季盤點資料庫中的戶政資料，並且於季末加密備份資料，維護資料完整性。
- 9.能源署指派之專員應建立個人資料安全維護計畫，並依計畫執行，落實資料安全之維護。

(二)資料銷毀程序

- 1.儲存於資訊系統資料庫之戶政資料，於各鄉（鎮、市、區）公所辦理年度補助業務完畢後，且確認無保存必要後刪除資料檔案，並確認其資料檔案無法復原，但其保存年限不得超過5年，保存年限屆滿前，應由能源署專責人員奉能源署權責主管核定後立即銷毀，銷毀紀錄應保留5年備查。
- 2.自戶政資訊連結作業取得之戶籍資料原始檔，應於自取得日起屆滿9個月後，由能源署專責人員奉能源署權責主管核定後立即銷毀，其銷毀過程亦應記錄並保留5年備查。
- 3.鄉（鎮、市、區）公所及村（里）辦公處保存之紙本形式補助名冊，屬會計法規定之會計原始憑證文件，其相關銷毀程序由鄉（鎮、市、區）公所依會計法規定辦理，

且應銷毀至無法識別之程度，於銷毀前，應確實盤點並妥善保管。進行個人資料安全維護內部稽核時，內部稽核應包含鄉（鎮、市、區）公所及村（里）辦公處紙本形式補助名冊之盤點與銷毀情形，以落實資料安全。

六、個人資料風險評估及管理機制

- (一)依能源署規劃，針對民眾個人資料檔案運用方式（包含蒐集、運用、存取、保存、編輯、傳輸等）各項作業之風險分析進行風險評估及研擬風險處理對策。
- (二)資料管理及查詢紀錄保存於伺服器內，並且半年定期檢視產製相關報表檢視有無異常使用情形，報表經能源署指派之專員提送主管簽核後於能源署留存 5 年備查。

七、定期查核及稽核

- (一)能源署應每月抽查戶政資料使用狀況，每月抽查比率至少為 3%，每月抽查筆數不得少於 10 筆，查詢總筆數少於 10 筆者，應全部查核。查核人員應定期輪調，且不得連續 3 個月查核同一受查人員，受查人員亦不得連續 3 個月被同一查核人員進行查核，查核紀錄應至少保留 5 年備查。
- (二)承商應於每季，針對個人資料安全維護計畫執行情形進行稽核，其稽核之內容應包含資料盤點、風險評估、定期備份、掃毒、資訊系統本機登入稽核與密碼設定原則、防火牆防駭、資訊安全檢測等，其稽核紀錄應至少保留 5 年備查。
- (三)鄉（鎮、市、區）公所每半年應稽核內部（含村（里）辦公處）個人資料安全維護情形，並留存稽核紀錄至少 5 年，稽核紀錄並應報直轄市、縣（市）政府，並由該府每半年據以辦理外部稽核(書面稽核)轄內公所作業。直轄市、縣（市）政府並得辦理實地稽核。直轄市、縣（市）政府辦理轄內鄉（鎮、市、區）公所稽核之紀錄應至少保留 5 年，並且報能源署備查。
- (四)直轄市、縣（市）政府每半年應稽核內部資訊系統使用情形，並留存稽核紀錄至少 5 年，稽核紀錄並應報能源署，並由能源署每半年據以辦理外部稽核(書面稽核)直轄市、縣（市）政府作業。能源署並得辦理實地稽核。能源署辦理直轄市、縣（市）政府稽核之紀錄應至少保留 5 年。
- (五)能源署應每半年辦理承商維護及存取戶政資料稽核工作，並作成稽核紀錄，其稽核紀錄應至少保留 5 年備查。
- (六)能源署應每半年辦理內部資訊安全稽核與個資安全稽核，並作成稽核紀錄，其稽核紀錄應至少保留 5 年備查。
- (七)能源署應配合經濟部每半年辦理之外部資訊安全稽核作業，且其稽核紀錄應至少保留 5 年備查。

八、使用紀錄資料之保存

- (一)能源署指派之專員與涉及差價補助業務之業務人員均應簽署個人資料保密同意切結書，保密切結書格式除將配合能源署規定，亦簽送能源署留存備查。

- (二)資訊系統涉及戶政資料之存取紀錄，應由能源署指派之專員每季加密備份後燒錄至光碟，並提交能源署留存備查。前揭存取紀錄包含使用者帳號、查詢事由、日期等查詢紀錄，不包含查詢結果，惟查詢事由因包含戶政資料，故採去識別化(雜湊)處理後紀錄。
- (三)資訊系統使用紀錄，應留存 5 年，保存年限屆滿前，由能源署專責人員奉能源署權責主管核定後立即銷毀。

九、異常事故之預防、通報及應變機制

- (一)資訊系統需建置於符 ISO27001 認證之機房，且系統應採與維護端環境獨立之網域，並透過授權帳號、OTP 身份驗證、防火牆管理，由能源署指派之專員透過指定之連線位置進行資訊系統維護，資訊系統亦應定期更新最新病毒碼及掃毒與進行 Windows Update，並設置入侵偵測，以預防各類攻擊。
- (二)資訊系統之維護端環境需設置硬體防火牆以管控各連線端點，監控與記錄網路即時運作情況，作業系統應定期更新最新病毒碼及掃毒與進行 Windows Update，以預防各類攻擊。
- (三)如遇有資訊安全異常事故發生時，能源署指派之專員應立即進行緊急處置，避免事故擴大，並保留相關紀錄，並立即通報能源署資安及業務主辦單位處理。

十、相關法律責任

- (一)對於取得戶政資料之蒐集、處理及利用，違反個資法規定，致侵害當事人權益者，由經濟部、能源署、持有及使用機關（鄉（鎮、市、區）公所（含村（里）辦公處））負同法第二十八條及第三十一條國家賠償責任。
- (二)意圖為自己或第三人不法之利益或損害他人之利益，或無故洩漏個人資料，或有其他違法或重大不當之行為而洩漏戶政資料者，除依法負民事及個資法之刑事責任外，應由人員隸屬機關議處行為人之行政責任。
- (三)管理人員未善盡管理之責，致未經授權之人，或因職務調整、離職或退休等原因已無使用戶政資料權限之人，不當取得戶政資料，致當事人權利受損者，應由人員隸屬機關議處管理人員之行政責任。
- (四)承商因執行契約書約定之受委託業務而違反個資法、個資法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。
- (五)如違反其他法律規定，依其規定追究責任。